

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 04-086135

(43)Date of publication of application : 18.03.1992

---

(51)Int.Cl.

H04L 9/06

H04L 9/14

---

(21)Application number : 02-201722

(71)Applicant : SHARP CORP

(22)Date of filing : 30.07.1990

(72)Inventor : HIRAIDE JUNJI  
TADA JUNJI

---

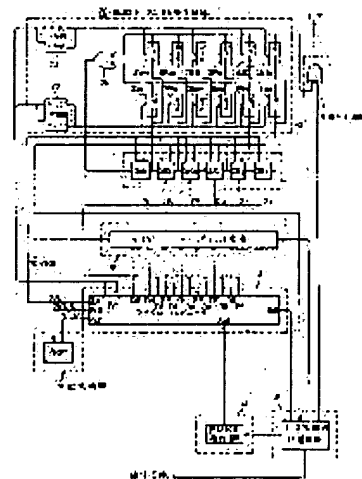
## (54) PRIVACY CALL DEVICE

### (57)Abstract:

PURPOSE: To enhance the privacy call performance by decoding a data based on the result of decoding of an address data ciphered by a pseudo random signal.

CONSTITUTION: An address data included in a signal from a communication line in the case of reception is fed to a microcomputer 6 via a serial/parallel conversion circuit 10 from a changeover circuit 8. Then the address data is fed to a storage circuit 3 from the microcomputer 6 to read relevant initial value data D1-D6, a stage number setting data and a tap position setting data. A decoding circuit 11 uses a pseudo random signal to decode accurately the ciphered data from the changeover circuit 8 and outputs the resulting data.

Thus, it is not required for the receiver side to enter a signal key, and the sender side revises freely a cryptographic key and the secrecy of the communication is sufficiently kept.



⑨ 日本国特許庁(JP)

⑩ 特許出願公開

⑪ 公開特許公報(A) 平4-86135

⑫ Int. Cl.<sup>9</sup>

識別記号

庁内整理番号

⑬ 公開 平成4年(1992)3月18日

H 04 L 9/06  
9/14

7117-5K H 04 L 9/02

Z

審査請求 未請求 請求項の数 2 (全12頁)

⑭ 発明の名称 秘話装置

⑮ 特 願 平2-201722

⑯ 出 願 平2(1990)7月30日

⑰ 発 明 者 平 出 順 二 大阪府大阪市阿倍野区長池町22番22号 シャープ株式会社  
内

⑱ 発 明 者 多 田 順 次 大阪府大阪市阿倍野区長池町22番22号 シャープ株式会社  
内

⑲ 出 願 人 シャープ株式会社 大阪府大阪市阿倍野区長池町22番22号

明 組 書

1 発明の名称

秘 話 装 置

2. 特許請求の範囲

(1) 送信側には、

シフトレジスタを使用して構成される第1の疑似ランダム信号発生回路と、

暗号鍵を設定する暗号鍵設定手段と、

上記第1の疑似ランダム信号発生回路の初期値データ、段数設定データおよびアップ位置設定データ等の初期設定データを記憶した第1の記憶回路と、

上記暗号鍵設定手段からの暗号鍵に外したアドレスデータによって上記第1の記憶回路から上記初期設定データを読み出して上記第1の疑似ランダム信号発生回路を設定する第1の制御手段と、

上記第1の疑似ランダム信号発生回路の出力信号によって入力データを暗号化する暗号化回路とが備えられ、

上記暗号化回路の出力データおよび上記アドレスデータが送信され、

受信側には、

上記第1の疑似ランダム信号発生回路と同じ構成の第2の疑似ランダム信号発生回路と、

上記第1の記憶回路と同じ内容を記憶した第2の記憶回路と、

受信した上記アドレスデータによって上記第2の記憶回路から上記初期設定データを読み出して上記第2の疑似ランダム信号発生回路を設定する第2の制御手段と、

上記第2の疑似ランダム信号発生回路の出力信号によって受信したデータを復号化する復号化回路とが備えられることを特徴とする秘話装置、

(2) 送信側には、

第1の疑似ランダム信号発生回路と、

初期設定データが固定値とされる第2の疑似ランダム信号発生回路と、

暗号鍵を設定する暗号鍵設定手段と、

上記第1の疑似ランダム信号発生回路の初期値

定データを記憶した第1の記憶回路と、

上記暗号設定手段からの暗号鍵に対応したアドレスデータによって上記第1の記憶回路から上記初期設定データを読み出して上記第1の疑似ランダム信号発生回路を設定する第1の制御手段と、

上記第1の疑似ランダム信号発生回路の出力信号によって入力データを暗号化する第1の暗号化回路と、

上記第2の疑似ランダム信号発生回路の出力信号によって上記アドレスデータを暗号化する第2の暗号化回路とが備えられ、

第1および第2の暗号化回路の出力データが送信され、

受信側には、

上記第1および第2の疑似ランダム信号発生回路とそれぞれ同じ構成の第3および第4の疑似ランダム信号発生回路と、

上記第1の記憶回路と同じ内容を記憶した第2の記憶回路と、

上記第4の疑似ランダム信号発生回路によって

受信した上記第2の暗号化回路の出力データを復号化する第1の復号化回路と、

上記第1の復号化回路より出力されるアドレスデータによって上記第2の記憶回路から上記初期設定データを読み出して上記第3の疑似ランダム信号発生回路を設定する第2の制御手段と、

上記第3の疑似ランダム信号発生回路の出力信号によって受信した上記第1の暗号化回路の出力データを復号化する第2の復号化回路とが備えられることを特徴とする秘密装置。

### 3. 発明の詳細な説明

#### 〔産業上の利用分野〕

この発明は、例えば有線あるいは無線デジタル通信に使用して好適な秘話装置に関する。

#### 〔従来の技術〕

通信において、通信内容が秘密である場合には秘話通信を行なう必要がある。この場合、送信側では、通常データ（平文）が暗号化され、この暗号化データ（暗号文）が送信される。そして、受

信側では、この暗号文が平文に復号化される。

従り図は、従来の秘話装置を示している。

同図において、送信側では、平文が暗号化回路13に供給されて暗号鍵15に応じて暗号文に変換される。この暗号化回路13からの暗号文は、有線または無線の通信経路を介して、受信側に供給される。また、受信側では、暗号文が復号化回路14に供給されて復号鍵16に応じて平文に変換される。

#### 〔発明が解決しようとする課題〕

第9図例によれば、送信側および受信側が、暗号化および復号化のために、例えば同一の鍵を所有する必要がある。そのため、送信側では暗号鍵を自由に変更することができなかった。しかし、通信の秘密を確保するには、暗号鍵を度々変更する必要がある。

そこで、本出願人は、先に、暗号鍵を自由に変更できる秘話装置を提案した（特開平1-70200号）。以下、この秘話装置について説明する。

第6図は送信側のブロック図である。

同図において、20は疑似ランダム信号発生回路であり、この疑似ランダム信号発生回路20は、6段のシフトレジスタSR1～SR6の縦続接続段1と、この縦続接続段1の傳遞路を選択する切り替え回路2とで構成される。

縦続接続段1のシフトレジスタSR1～SR6のロードおよびシフト装置は、制御手段であるマイクロコンピュータからの制御信号S/LOADによって制御される。制御信号S/LOADがロード状態のとき、シフトレジスタSR1～SR6には、マイクロコンピュータからの初期値データD1～D6がロードされる。なお、これらシフトレジスタSR1～SR6はクロックCKに同期して動作するようにされる。

切り替え回路2は、ゲートおよびインバータで構成される。すなわち、アンドゲート21にはシフトレジスタSR5の出力信号が供給されると共に、マイクロコンピュータからの制御データDTが供給される。また、アンドゲート23にはシフトレジスタSR1の出力信号が供給されると共に、制御

データD7がインバータ22を介して供給される。そして、これらアンドゲート21および23の出力信号がオアゲート24に供給される。したがって、制御データD7がハイレベルかローレベルかに応じて、オアゲート24からはシフトレジスタSR1またはSR5の出力信号が出力される。

また、エクスクルーシブオアゲート25にはオアゲート24の出力信号が供給されると共に、シフトレジスタSR6の出力信号が供給される。そして、このエクスクルーシブオアゲート25の出力信号はシフトレジスタSR1に帰還される。したがって、シフトレジスタSR1～SR6がシフト動作をするとき、シフトレジスタSR6からは初期値データD1～D6および切り替え回路2の選択に応じた疑似ランダム信号が出力される。

また、5は暗号鍵設定手段であり、この暗号鍵設定手段5は、ハイレベルまたはローレベルを選択する7個の推定スイッチで構成される。これら7個の推定スイッチの一端は電源端子に接続され、その他端はマイクロコンピュータ6の端子P11～

P17に接続される。

また、3は例えばROM(リードオンリーメモリ)で構成される記憶回路であり、この記憶回路3には縦横検出線1のシフトレジスタSR1～SR6に供給される初期値データD1～D6と、切り替え回路2に供給される制御データD7とが複数記憶されている。

この場合、暗号鍵設定手段5で設定された暗号鍵に応じたアドレスデータがマイクロコンピュータ6より記憶回路3に供給され、対応する初期値データD1～D6および制御データD7が読み出される。そして、この初期値データD1～D6および制御データD7はマイクロコンピュータ6の端子P01～P07を介してシフトレジスタSR1～SR6および切り替え回路2に供給され、これにより疑似ランダム信号発生回路20が初期値設定される。

また、マイクロコンピュータ6からのアドレスデータはパラレル/シリアル変換回路4でシリアル信号に変換されて出力される。

また、7はエクスクルーシブオアゲートで構成

される暗号化回路であり、この暗号化回路7には、疑似ランダム信号発生回路20からの疑似ランダム信号と、データ発生手段(図示せず)からのシリアルデータ(例えば、音声データ)とが供給されて、シリアルデータは暗号化される。

また、8はデータ/制御信号切り替え回路であり、この切り替え回路8には変換回路4より出力されるアドレスデータ、暗号化回路7より出力される暗号化データおよび同期信号発生回路9からの同期信号が供給される。そして、マイクロコンピュータ6の制御により、これらの信号はクロックCKに同期して切り替えられ、有線または無線の通信回路に出力される。第8図はその通信信号の構成例を示している。

このように、送信側では、暗号鍵設定手段5による暗号鍵の決定に応じて、データが暗号化され、同期信号およびアドレス信号と共に、通信回路に出力される。

第7図は、受信側のブロック図である。この第7図において、第6図と対応する部分には同一符

号を付して示している。

同図において、通信回路からの信号はデータ/制御信号切り替え回路8を介して同期信号検出回路12に供給され、この同期信号検出回路12で検出される同期信号(第8図参照)はマイクロコンピュータ6に供給される。

また、切り替え回路8には、マイクロコンピュータ6より同期信号に応じて制御信号およびクロックCKが供給される。そして、通信回路からの信号に含まれるアドレスデータは切り替え回路8よりシリアル/パラレル変換回路10でパラレル信号に変換されたのちマイクロコンピュータ6に供給される。そして、このアドレスデータはマイクロコンピュータ6より記憶回路3に供給され、対応する初期値データD1～D6および制御データD7が読み出される。そして、この初期値データD1～D6および制御データD7はマイクロコンピュータ6の端子P01～P07を介して疑似ランダム信号発生回路20のシフトレジスタSR1～SR6および切り替え回路2に供給される。これにより疑似

ランダム信号発生回路20が初期設定される。

この場合、受信側および送信側の記憶回路3の記憶内容は同じであると共に、受信側および送信側の疑似ランダム信号発生回路20は同じ構成であるので、受信側の疑似ランダム信号発生回路20からは、送信側と同様の疑似ランダム信号が発生される。

また、11はエクスクルーシブオアゲートで構成される復号化回路である。この復号化回路11には、疑似ランダム信号発生回路20からの疑似ランダム信号と、切り替え回路8からの暗号化データとが供給され、暗号化データは復号化されて出力される。

このように第6図および第7図に示す協話装置によれば、受信側で復号鍵を入力する必要はなく、送信側で暗号鍵を自由に変更することができる。

ところで、暗号は常に第三者により解読される危険性を持っており、より秘密性の高い装置が要求される。

そこで、この発明では、秘密性をさらに高めた

協話装置を提供するものである。

#### 【問題を解決するための手段】

第1の発明に係る協話装置は以下のように構成される。

送信側には、シフトレジスタを使用して構成される第1の疑似ランダム信号発生回路と、暗号鍵を設定する暗号鍵設定手段と、第1の疑似ランダム信号発生回路の初期値データを、初期設定データおよびタップ位置設定データ等の初期設定データを記憶した第1の記憶回路と、暗号鍵設定手段からの暗号鍵に対応したアドレスデータによって第1の記憶回路から初期設定データを読み出して第1の疑似ランダム信号発生回路を設定する第1の制御手段と、第1の疑似ランダム信号発生回路の出力信号によって入力データを暗号化する暗号化回路とが備えられ、暗号化回路の出力データおよびアドレスデータが送信される。

受信側には、第1の疑似ランダム信号発生回路と同じ構成の第2の疑似ランダム信号発生回路と、第1の記憶回路と同じ内容を記憶した第2の記憶

回路と、受信したアドレスデータによって第2の記憶回路から初期設定データを読み出して第2の疑似ランダム信号発生回路を設定する第2の制御手段と、第2の疑似ランダム信号発生回路の出力信号によって受信したデータを復号化する復号化回路とが備えられる。

第2の発明に係る協話装置は、以下のように構成される。

送信側には、第1の疑似ランダム信号発生回路と、初期設定データが固定値とされる第2の疑似ランダム信号発生回路と、暗号鍵を設定する暗号鍵設定手段と、第1の疑似ランダム信号発生回路の初期設定データを記憶した第1の記憶回路と、暗号鍵設定手段からの暗号鍵に対応したアドレスデータによって第1の記憶回路から初期設定データを読み出して第1の疑似ランダム信号発生回路を設定する第1の制御手段と、第1の疑似ランダム信号発生回路の出力信号によって入力データを暗号化する第1の暗号化回路と、第2の疑似ランダム信号発生回路の出力信号によってアドレスデー

タを暗号化する第2の暗号化回路とが備えられ、第1および第2の暗号化回路の出力データが送信される。

受信側には、第1および第2の疑似ランダム信号発生回路とそれぞれ同じ構成の第3および第4の疑似ランダム信号発生回路と、第1の記憶回路と同じ内容を記憶した第2の記憶回路と、第4の疑似ランダム信号発生回路によって受信した第2の暗号化回路の出力データを復号化する第1の復号化回路と、第1の復号化回路より出力されるアドレスデータによって第2の記憶回路から初期設定データを読み出して第3の疑似ランダム信号発生回路を設定する第2の制御手段と、第3の疑似ランダム信号発生回路の出力信号によって受信した第1の暗号化回路の出力データを復号化する第2の復号化回路とが備えられる。

#### 【作 用】

第1の発明においては、疑似ランダム信号発生回路の段数、タップ位置を自由に設定することができ、秘密性をより高めることが可能となる。

第2の発明においては、アドレスデータが疑似ランダム信号によって暗号化され、このアドレスデータの復号結果に基づいて、データの復号化が行なわれるので、秘匿性をより高めることができる。

#### 【実施例】

以下、図面を参照しながら、第1の発明の実施例について説明する。

第1図は、送信側のブロック図である。この第1図において、第6図と対応する部分には同一符号を付し、その詳細説明は省略する。

本例においては、暗号鍵設定手段5からの暗号鍵は演算回路で構成される暗号鍵変換回路17を介してマイクロコンピュータ6に供給される。変換回路17にはマイクロコンピュータ6より通信回数のデータが供給され、暗号鍵設定手段5より供給される暗号鍵は通信ごとに異なるように変更される。

このように変更するための演算処理例としては、通信ごとに「1」を加算していくというような簡

単なものから、PN発生回路によるスワランブル化、乗算、除算や各種演算による複雑なものまで考えられる。

また本例において、疑似ランダム信号発生回路20は、6段のシフトレジスタSR1～SR6の縦横接続段1と、使用するシフトレジスタの段数および循環のためのクランプ位置を切り替える切り替え回路2'とで構成される。シフトレジスタSR1～SR6のロードおよびシフト状態は、第6図例と類似に、マイクロコンピュータ6からの制御信号S/Lによって制御される。

シフトレジスタSR1～SR6の出力信号は、それぞれ接続スイッチSW11～SW16を介してエクスクルーシブオアゲート26に供給されると共に、それぞれ接続スイッチSW21～SW26を介してエクスクルーシブオアゲート26および暗号化回路7に供給される。そして、エクスクルーシブオアゲート26の出力信号は、シフトレジスタSR1に供給される。

接続スイッチSW11～SW16のオンオフは、そ

れぞれクランプ切り替え用デコード27の出力信号によって制御される。つまり、いずれか1つがオンとされ、循環のためのクランプ位置が決定される。

接続スイッチSW21～SW26のオンオフは、それぞれ段数切り替え用デコード28の出力信号によって制御される。つまり、いずれか1つがオンとされ、使用されるシフトレジスタの段数が設定される。

また本例において、記憶回路3には、縦横接続段1のシフトレジスタSR1～SR6に供給される初期値データD1～D6、段数切り替え用デコード28に供給される段数設定データおよびクランプ切り替え用デコード27に供給されるクランプ位置設定データが複数組記憶されている。

以上の構成において、送信をする際には、変換回路17でもって変更された暗号鍵に応じたアドレスデータがマイクロコンピュータ6より記憶回路3に供給され、対応する初期値データD1～D6、段数設定データおよびクランプ位置設定データが読み出される。

そして、初期値データD1～D6はマイクロコンピュータ6の端子P01～P06を介してシフトレジスタSR1～SR6に供給され、この初期値データD1～D6がシフトレジスタSR1～SR6にロードされて、初期値がセットされる。

段数設定データはマイクロコンピュータ6の端子P07を介して段数切り替え用デコード28に供給され、このデコード28からは段数設定データに対応した信号が出力され、これにより接続スイッチSW21～SW26のオンオフが制御されて、段数が設定される。

クランプ位置設定データはマイクロコンピュータ6の端子P07を介してクランプ切り替え用デコード27に供給され、このデコード27からはクランプ位置設定データに対応した信号が出力され、これにより接続スイッチSW11～SW16のオンオフが制御されて、クランプ位置が設定される。

その結果、疑似ランダム信号発生回路20からは、シフトレジスタSR1～SR6にセットされた初期値、設定された段数および設定されたクランプ

位置に応じた疑似ランダム信号が出力され、暗号化回路7では、この疑似ランダム信号をもってデータが暗号化される。

なお、その他の部分に関しては、第6図例と同様であり、説明は省略する。

次に、第2図は、受信側のブロック図である。この第2図において、第7図と対応する部分には同一符号を付し、その詳細説明は省略する。

本例において、疑似ランダム信号発生回路20および記憶回路3は、第1図の送信側と同様に構成される。

以上の構成において、受信をする際、通信回路からの信号に含まれるアドレスデータは、切り替え回路8よりシリアル/パラレル変換回路10を介してマイクロコンピュータ6に供給される。そして、このアドレスデータは、マイクロコンピュータ6より記憶回路3に供給され、対応する初期値データD1~D6、段数設定データおよびタップ位置設定データが読み出される。

そして、初期値データD1~D6はマイクロコン

ピュータ6の端子P01~P06を介してシフトレジスタSR1~SR6に供給され、この初期値データD1~D6がシフトレジスタSR1~SR6にロードされて、初期値がセットされる。

段数設定データはマイクロコンピュータ6の端子P07を介して段数切り替え用デコード28に供給され、このデコード28からは段数設定データに対応した信号が出力され、これにより接続スイッチSW21~SW26のオンオフが制御されて、段数が設定される。

タップ位置設定データはマイクロコンピュータ6の端子P07を介してタップ切り替え用デコード27に供給され、このデコード27からはタップ位置設定データに対応した信号が出力され、これにより接続スイッチSW11~SW16のオンオフが制御されて、タップ位置が設定される。

この場合、受信側および送信側の記憶回路3の記憶内容は同じであると共に、受信側および送信側の疑似ランダム信号発生回路20は同じ構成であるので、疑似ランダム信号発生回路20は送信

側と同様に設定され、送信側と同様の疑似ランダム信号が発生される。

そのため、復号化回路11では、この疑似ランダム信号をもって切り替え回路8からの暗号化データが正確に復号化され、データが出力される。

なお、その他の部分に関しては、第7図例と同様であり、説明は省略する。

このように第1図および第2図に示す秘密装置によれば、受信側で復号鍵を入力する必要はなく、送信側で暗号鍵を自由に変更することができる。

また、暗号鍵に応じて疑似ランダム信号発生回路20の初期値だけでなく、ハード構成(段数、タップ位置)も変更されるので、秘密性を高めることができる。

さらに、暗号鍵は変換回路17で送信側に異なるように変更されるので、ユーザーを誤らせることなく、通信の秘密を充分に保持することができる。

次に、第2の発明の一実施例について説明する。第3図は、送信側のブロック図である。この第

3図において、第6図と対応する部分には同一符号を付し、その詳細説明は省略する。

本例において、暗号鍵設定手段9からの暗号鍵は演算回路で構成される暗号鍵変換回路17を介してマイクロコンピュータ6に供給される。変換回路17にはマイクロコンピュータ6より通信回路のデータが供給され、暗号鍵設定手段9より供給される暗号鍵は送信ごとに異なるように変更される。

このように変更するための演算処理例としては、通信ごとに「1」を加重していくというような簡単なものから、PN発生回路によるスクランブル化、乗算、除算や各種演算による複雑なものまで考えられる。

また、本例においては、疑似ランダム信号発生回路20の他に、同様の構成とされた疑似ランダム信号発生回路20'が設けられる。連続接続段1のシフトレジスタSR1~SR6のロードおよびシフト状態は、マイクロコンピュータ6からの制御信号Sノシによって制御される。

また、この疑似ランダム信号発生回路20'の初期設定は、マイクロコンピュータ6の端子P01~P06より魔鏡接続段1のシフトレジスタSR1~SR6に初期値データD1'~D6'が供給されてセットされると共に、マイクロコンピュータ6の端子P07より切り替え回路2に制御データD7'が供給されて格連のためのタップ位置が設定される。この場合、初期値データD1'~D6'、制御データD7'は固定値とされる。

疑似ランダム信号発生回路20'からの疑似ランダム信号は、エクスクルーシブオアゲートで構成される暗号化回路7'に供給される。この暗号化回路7'には、パラレル/シリアル変換回路4でシリアルデータとされたアドレスデータが供給され、疑似ランダム信号をもって暗号化される。そして、この暗号化回路7'からの暗号化されたアドレスデータはデータ/制御信号切り替え回路8に供給される。

以上の構成において、送信をする際には、変換回路17をもって変更された暗号鍵に応じたアド

レスデータがマイクロコンピュータ6より記憶回路3に供給され、対応する初期値データD1~D6および制御データD7が読み出される。そして、この初期値データD1~D6および制御データD7は、マイクロコンピュータ6の端子P01~P07を介して疑似ランダム信号発生回路20のシフトレジスタSR1~SR6および切り替え回路2に供給され、これにより疑似ランダム信号発生回路20が初期設定される。

その結果、疑似ランダム信号発生回路20からは、シフトレジスタSR1~SR6にセットされた初期値、切り替え回路2で設定されたタップ位置に応じた疑似ランダム信号が出力され、暗号化回路7では、この疑似ランダム信号をもってデータが暗号化され、この暗号化データは切り替え回路8に供給される。

また、固定値である初期値データD1'~D6'および制御データD7'がマイクロコンピュータ6の端子P01~P07を介して疑似ランダム信号発生回路20'のシフトレジスタSR1~SR6および

切り替え回路2に供給され、これにより疑似ランダム信号発生回路20'が初期設定される。

その結果、疑似ランダム信号発生回路20'からは、シフトレジスタSR1~SR6にセットされた初期値、切り替え回路2で設定されたタップ位置に応じた疑似ランダム信号が出力され、暗号化回路7'では、この疑似ランダム信号をもってアドレスデータが暗号化され、この暗号化されたアドレスデータは切り替え回路8に供給される。

したがって、切り替え回路8から通信回路には、第5図に示すような通信信号が出力される。

なお、その他の部分に関しては、第6図例と同様であり、説明は省略する。

次に、第4図は、受信側のブロック図である。この第4図において、第7図と対応する部分には同一符号を付し、その詳細説明は省略する。

本例においては、送信側と同様の構成の疑似ランダム信号発生回路20'が設けられる。魔鏡接続段1のシフトレジスタSR1~SR6のロードおよびシフト状態は、マイクロコンピュータ6から

の制御信号S/Lによって制御される。この疑似ランダム信号発生回路20'の初期設定は、固定の初期値データD1'~D6'および制御データD7'がマイクロコンピュータ6の端子P01~P07よりシフトレジスタSR1~SR6および切り替え回路2に供給されて行なわれる。

疑似ランダム信号発生回路20'からの疑似ランダム信号は、エクスクルーシブオアゲートで構成される復号化回路11'に供給される。この復号化回路11'には、切り替え回路8より暗号化されたアドレスデータが供給される。そして、復号化回路11'の出力信号は、シリアル/パラレル変換回路10に供給される。

以上の構成において、受信をする際には、通信回路からの信号に含まれる同期信号に基づいて、マイクロコンピュータ6の端子P01~P07の端子より疑似ランダム信号発生回路20'に初期値データD1'~D6'および制御データD7'が供給されて初期設定される。

そして、通信回路からの信号に含まれる暗号化



されたアドレスデータは、切り替え回路8より復号化回路11'に供給されて、疑似ランダム信号発生回路20'からの疑似ランダム信号をもって復号化される。

この場合、受信側および送信側の疑似ランダム信号発生回路20'は同じ構成であり、固定の初期値データD1'～D6'および制御データD7'で初期設定されるので、受信側の疑似ランダム信号発生回路20'からは送信側と同様の疑似ランダム信号が発生される。そのため、復号化回路11'では正確に復号化され、アドレスデータが出力される。

復号化回路11'からのアドレスデータは、シリアル/パラレル変換回路10を介してマイクロコンピュータ6に供給される。そして、このアドレスデータは、マイクロコンピュータ6より記憶回路3に供給され、対応する初期値データD1～D6および制御データD7が読み出され、マイクロコンピュータ6の端子P01～P07を介して疑似ランダム信号発生回路20に供給されて初期設定される。

さらに、暗号鍵は変換回路17で通信路に異なるように変更されるので、ユーザーを偽らせることなく、通信の秘密を充分に保持することができる。

なお、上述実施例においては、変換回路17のシフトレジスタの段数は6段とされたものであるが任意の段数とすることができる。

また、第3図例および第4図例においては、疑似ランダム信号発生回路20および20'は同様の構成とされたものであるが、異なる構成としてもよい。

#### [ 発明の効果 ]

以上説明したように、第1の発明によれば、受信側で復号鍵を入力する必要はなく、送信側で暗号鍵を自由に変更することができると共に、暗号鍵に応じて疑似ランダム信号発生回路20の初期値だけでなく、ハード構成（段数、タップ位置）も変更されるので、通信の秘密を充分に保持することができる。

また、第2の発明によれば、受信側で復号鍵を

る。

そして、通信回路からの信号に含まれる暗号化データは切り替え回路8より復号化回路11に供給されて、疑似ランダム信号発生回路20からの疑似ランダム信号をもって復号化される。

この場合、受信側および送信側の記憶回路3の記憶内容は同じであると共に、受信側および送信側の疑似ランダム信号発生回路20は同じ構成であるので、疑似ランダム信号発生回路20は送信側と同様に初期設定され、送信側と同様の疑似ランダム信号が発生される。そのため、復号化回路11では正確に復号化され、データが出力される。

なお、その他の部分に関しては、第7図例と同様であり、説明は省略する。

このように第3図および第4図に示す秘匿装置によれば、受信側で復号鍵を入力する必要はなく、送信側で暗号鍵を自由に変更することができる。

また、アドレスデータも暗号化されて送信されるので、受信側ではその復号化が必要となり、秘匿性を高めることができる。

入力する必要はなく、送信側で暗号鍵を自由に変更できると共に、アドレスデータも暗号化されて送信されるので、受信側ではその復号化が必要となり、通信の秘密を充分に保持することができる。

#### 4. 図面の簡単な説明

第1図および第2図は第1の発明の一実施例を示すブロック図、第3図および第4図は第2の発明の一実施例を示すブロック図、第5図はその通信信号の構成を示す図、第6図は秘匿装置の送信側のブロック図、第7図は秘匿装置の受信側のブロック図、第8図は通信信号の構成を示す図、第9図は従来の秘匿装置のブロック図である。

3・・・記憶回路

4・・・シリアル/パラレル変換回路

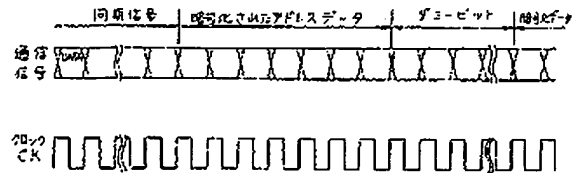
5・・・暗号鍵設定手段

6・・・マイクロコンピュータ

7、7'・・・暗号化回路

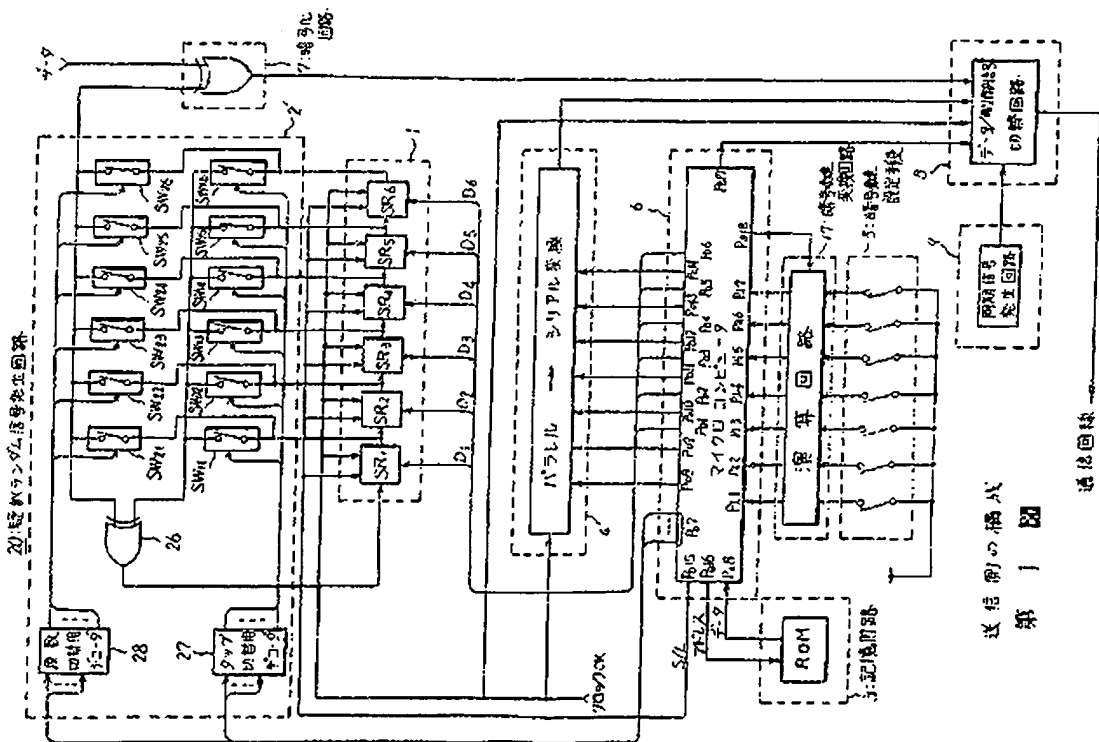
8・・・データ/制御信号切り替え回路

- 9 . . . 同期信号発生回路
- 10 . . . シリアル／パラレル変換回路
- 11.11 . . . 復号化回路
- 12 . . . 同期信号検出回路
- 17 . . . 符号変換回路
- 20. 20 . . . 連続ランダム信号発生回路

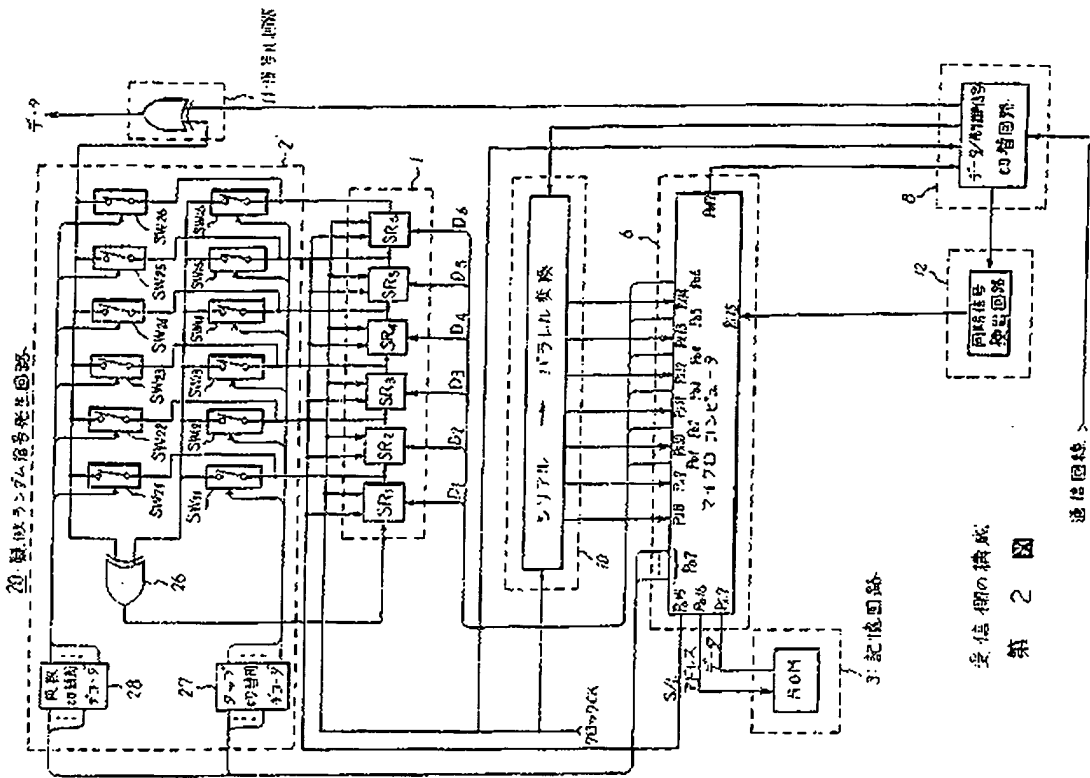


特許出願人 シマーズ株式会社  
代理人 弁護士 山口 邦夫

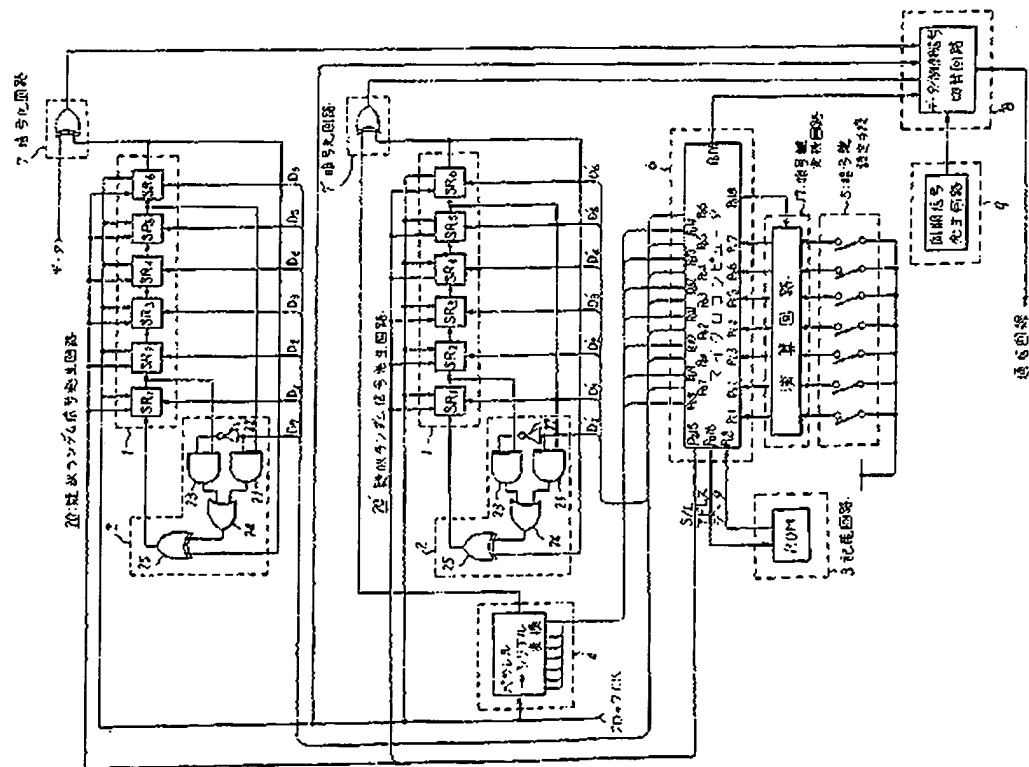
通信信号の一例  
第5図



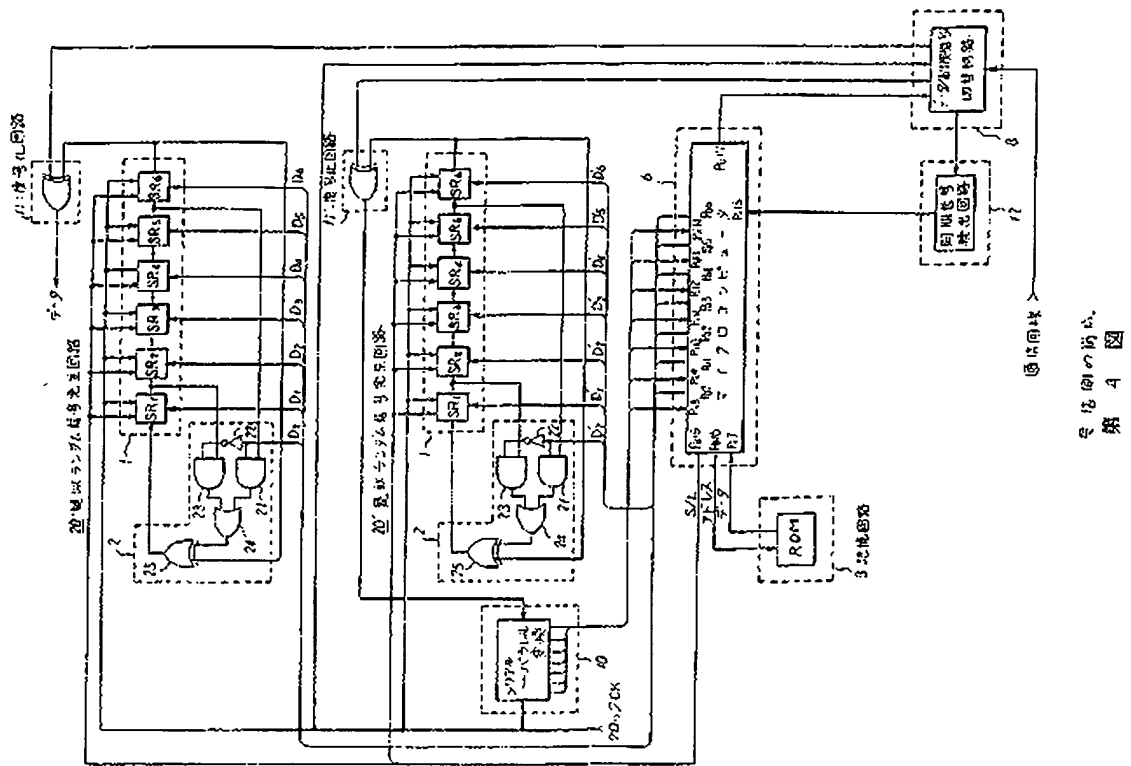
送信機の構成  
第1図



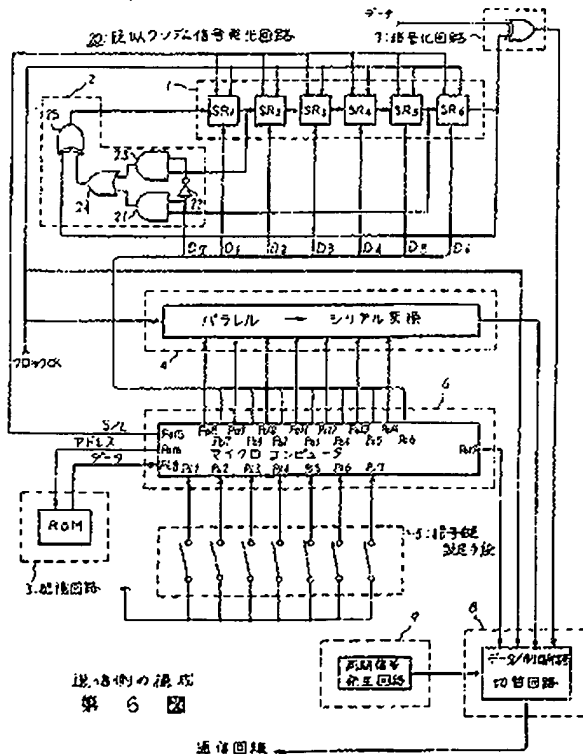
  
 〃  
 振



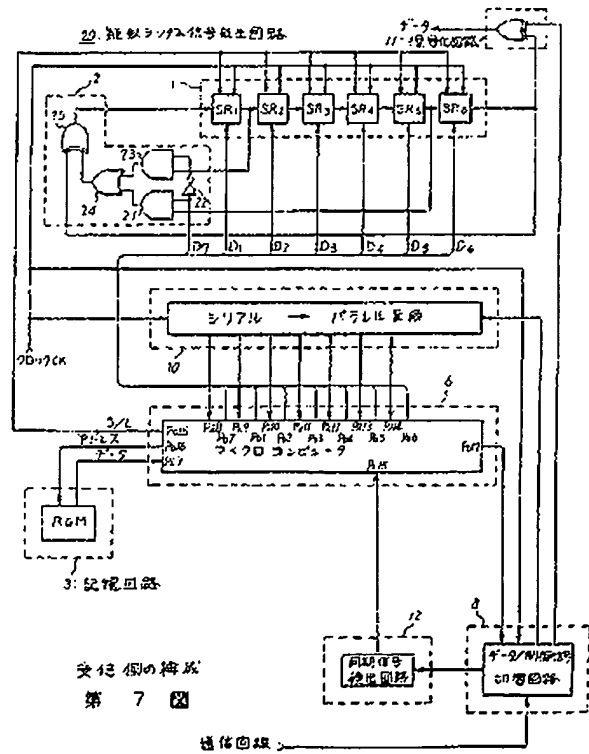
送 第 3 圖



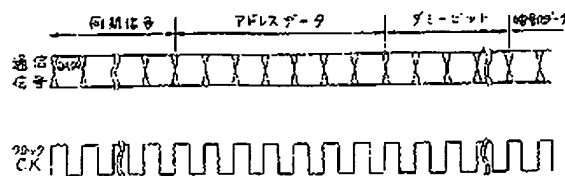
第4図



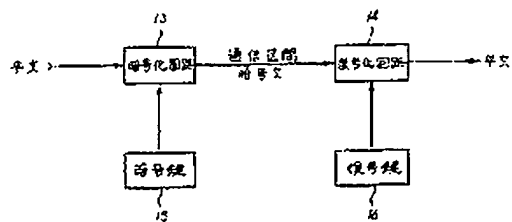
第6図



第7図



通信信号の一例  
第 8 図



従来例の構成図  
第 9 図